ESBWR Seminar – Instrumentation & Control (I&C)

September 15, 2006
Larry E. Fennern

Digital Control & Instrumentation

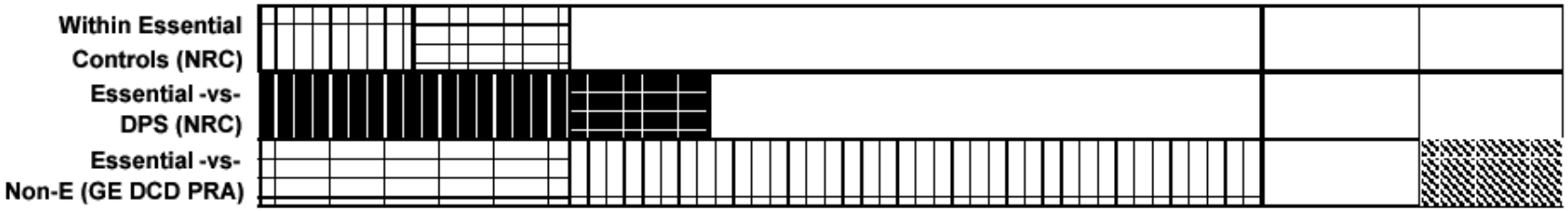
- Four divisions of Reactor Protection System (RPS) (Scram)
- Four divisions of Engineering Safety Features (e.g., ECCS)
- Four divisions of ATWS/SLCS
  (Anticipated Transients Without Scram/Standby Liquid Control System)
- Triple redundant controller for Diverse RPS and ECCS
- Triple redundant controllers for major nuclear process control
- Redundant controllers for investment protection and Balance of Plant (BOP) control

Digital Control & Instrumentation System (DCIS) Platform Families and Diversity

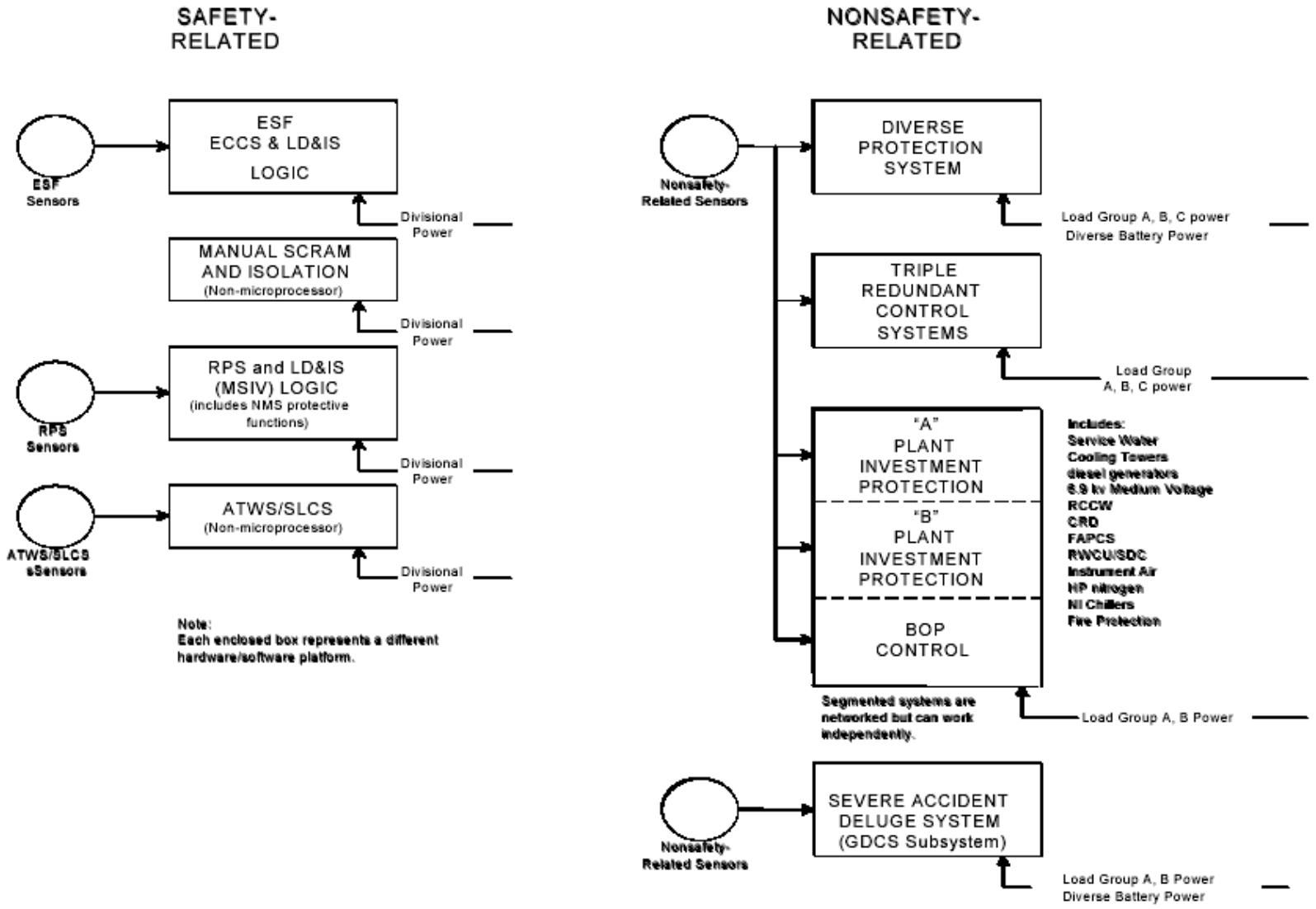
Safety	Safety-Related		Nonsafety-Related				
Category	E - DCIS		NE - DCIS				
System Families	RPS NMS	ECCS ESF	DPS	NUCLEAR CONTROL SYSTEMS	Balance of any NE-DCIS Systems	PCF	Severe Accident
Architecture	NUMAC Derived	Redundant	Triple Redundant	Triple Redundant	Dual Redundant	Workstations **	PLCs
Systems/ Subsystems	RPS LD&IS (MSIV) NMS ATWS/SLCS*	ICS SRV/DPV GDCS SLCS LD&IS (Non-MSIV)	RPS ECCS Backup	FWC, PAS (Automation SB&PC, T/G Control	PIP A, PIP B Balance Of Plant (Power Generation)	HMI, Alarms, SPDF, Historian, 3D-Monicore	Deluge System (GDCS Subsystem)

** Dual redundant as necessary

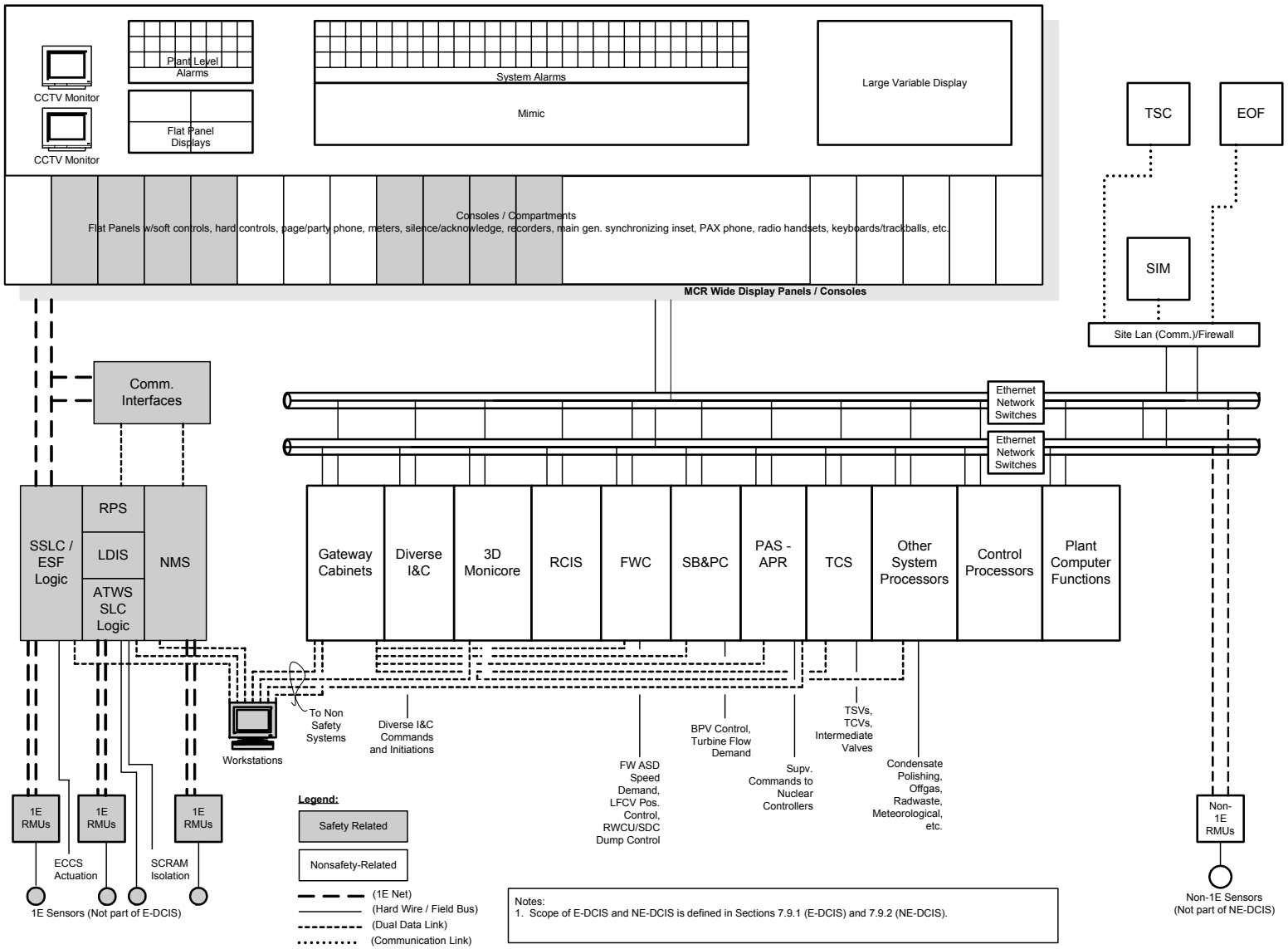
Diversity Strategy



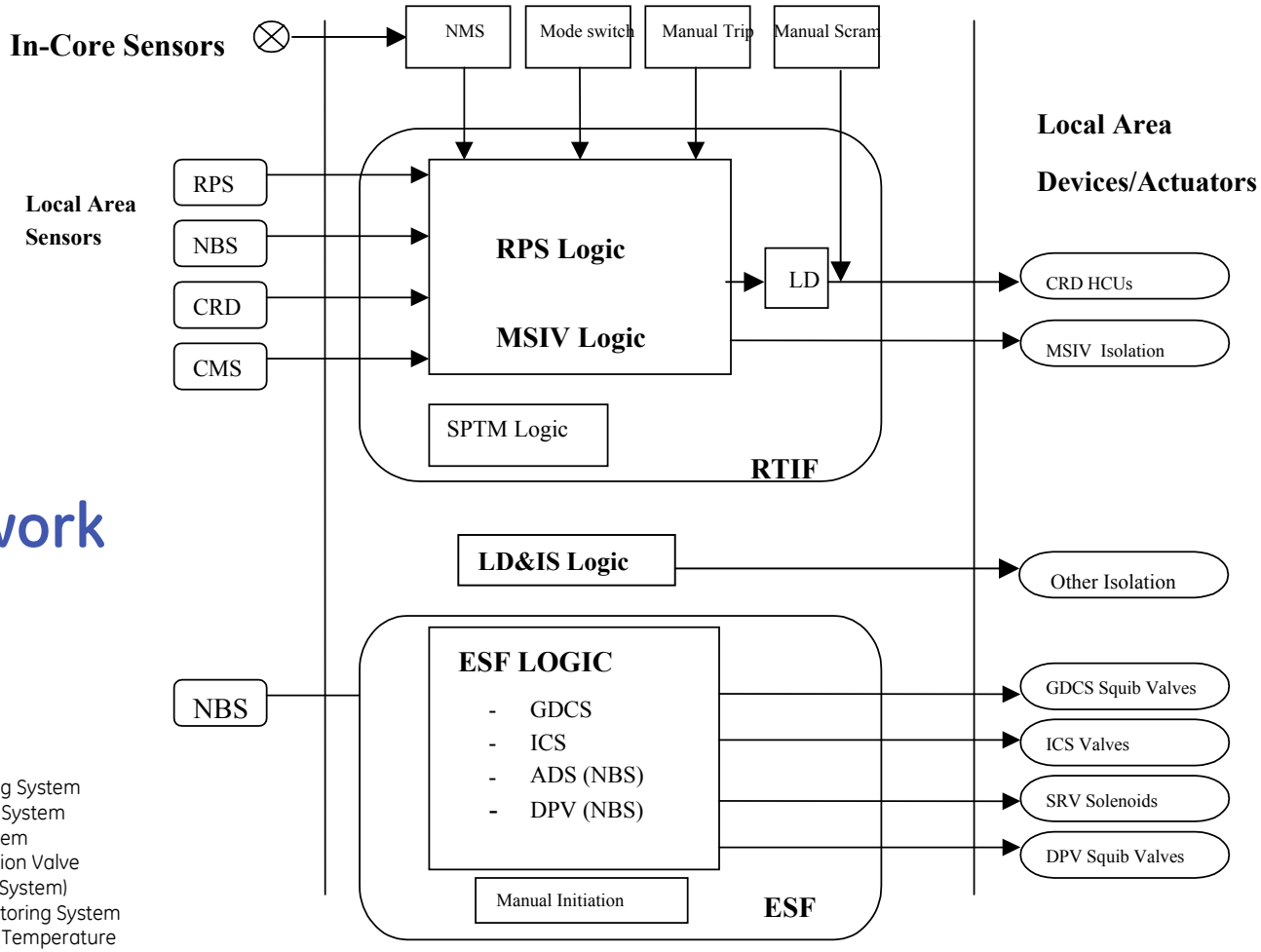
DCIS Power and Sensor Diversity



Overview of ESBWR I&C Systems Architect



SSLC System Framework



NMS = Neutron Monitoring System
RPS = Reactor Protection System
NBS = Nuclear Boiler System
MSIV = Main Steam Isolation Valve
CRD = Control Rod Drive (System)
CMS = Containment Monitoring System
SPTM = Suppression Pool Temperature Monitoring
RTIF = Reactor Trip & Isolation Function
LD&IS = Leak Detection & Isolation System
ESF= Engineered Safety Features
GDCS = Gravity Driven Cooling System
ICS = Isolation Condenser System
ADS = Automatic Depressurization System
SRV = Safety Relief Valve
DPV = Depressurization Valve
LD = Load Driver
HCU = Hydraulic Control Unit

1Local area sensors include:
RPS: turbine stop valve position, turbine CV oil pressure, turbine bypass valve position
NBS: MSIV position (for RTIF only), RPV pressure, water level
CRD: HCU accumulator charging water header pressure
CMS: drywell pressure
2Manual Scram interrupts power to the circuit.
3LD&IS resides in SSLC and shares sensors inputs with RTIP and ESF

ESBWR Safety System Logic Control (SSLC) Framework

- Each Subsystem has 4 digital safety-related Divisions (Class 1E)
- RPS is independent and separate from ESF Logics

Reactor Protection System

- Based on ABWR design
  - 2/4 logic
  - Fail safe
  - Deterministic
  - Diverse from ECCS
- Any two unbypassed same parameters exceeding limits always cause a scram with:
  - Any single logic failure
  - Any division of sensors bypass status
  - Any division of logic bypass status (independent from sensor bypass)
  - Any single power failure
  - Any possible main control room RPS control configuration
- Each division makes a per parameter trip decision
- Each division informs other divisions of its trip data (via communication module and isolated fiber optics)
- Each division makes a 2/4 per parameter decision to scram
- Two divisions of load drivers – each driven by four divisional trip outputs – control HCU scram solenoids

ESBWR Safety System Logic Control (SSLC) Framework

Engineering Safety Features Logics (SSLC/ESF)

- Based on ABWR design
  - 2/4 logic
  - Fail As-Is
  - Deterministic
  - Diverse from RPS
- Any two unbypassed same parameters exceeding limits always initiate ECCS with:
  - Any single logic failure
  - Any division of sensors bypass status
  - Any single power failure
- Each division makes a per parameter trip decision
- Each division informs other divisions of its trip data (via communication module and isolated fiber optics)
- Each division makes a dual 2/4 per parameter decision to initiate
- Each divisional redundant 2/4 logic drives an output load driver
- Redundant load drivers per division wired in series
- Design is single failure proof (logic and power) to actuate when required
- Design is single failure proof to prevent inadvertent actuation
- Any one of two (or four*) power divisions can actuate one of the two (or four*) actuators (SRV solenoid, GDCS or DPV squib valve) and open the valve *N-2 capable

Other Major ESBWR Safety-Related Systems

Neutron Monitoring System (NMS)

> Startup Range Neutron Monitor (SRNM)

– 12 SRNM detector assemblies assigned in 4 divisions

– Each divisional 2/4 logic final trip output sent to each of 4 RPS divisions

> Power Range Neutron Monitor (PRNM)

– LPRM: 64 LPRM assemblies with 4 detectors per assembly

– APRM: 256 LPRM detectors evenly assigned in 4 APRMs to represent average core power

– Each divisional 2/4 logic final trip output sent to each of 4 RPS divisions

Remote Shutdown System (RSS)

> Safety-related digital dual channels

> All safety and nonsafety systems MMI available to the operator from RSS

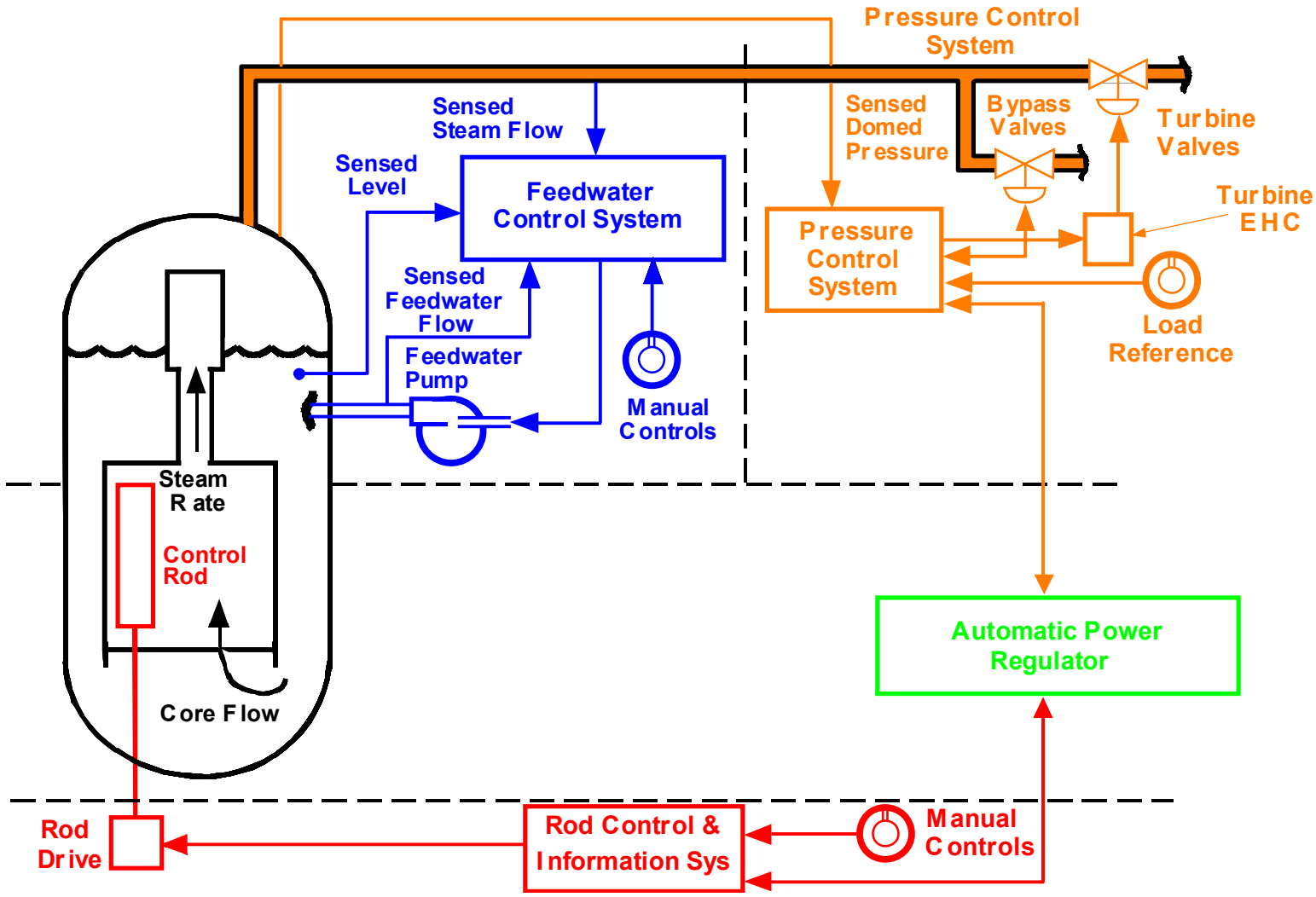
–If offsite power is available, normal heat sinks and injection systems can be operated

–If diesels are available the investment protection equipment can be operated

–If no AC power is available, safety systems (IC, ADS, GDCS etc) can be operated

> Automatic and manual RSS operation does not depend on main control room operation after it has been evacuated

ESBWR Key (Triply Redundant) Control Systems



Overview of ESBWR Major Control Systems

Nuclear Boiler System (NBS) Instrumentation

> Safety-related and Nonsafety-related sensors (RPV pressure and water level) for diverse application

– Independent for RPS, ECCS, and control systems

> Safety Relief Valves (SRVs) and Depressurization Valves (DPVs) for ECCS Application

– Initiation logics within SSLC

Rod Control and Information System (RC&IS)

> Control of control rods movement for reactor power level control.

> Nonsafety-related dual independent and separate channels.

> The automated thermal limit monitor (ATLM) automatically enforces fuel operating thermal limits minimum critical power ratio (MCPR) and maximum linear heat generation rate (MLHGR).

> Control rod position information display to plant operator in main control room

Feedwater Control System (FWCS)

> Triplicated redundant nonsafety-related I&C system.

> Automatically or manually regulates the feedwater flow into the reactor pressure vessel to maintain predetermined water level limits during transients and normal plant operating modes.

Overview of ESBWR Major Control Systems (Continued)

System Bypass and Pressure Control System (SBPC)

> Triplicated redundant nonsafety-related I&C system

> Controls reactor pressure during plant startup, power generation and shutdown modes of operation, by directly controlling the turbine bypass and indirectly controlling turbine control valve position by sending pressure regulation demand signals to the Turbine Control System - Electro-Hydraulic Control.

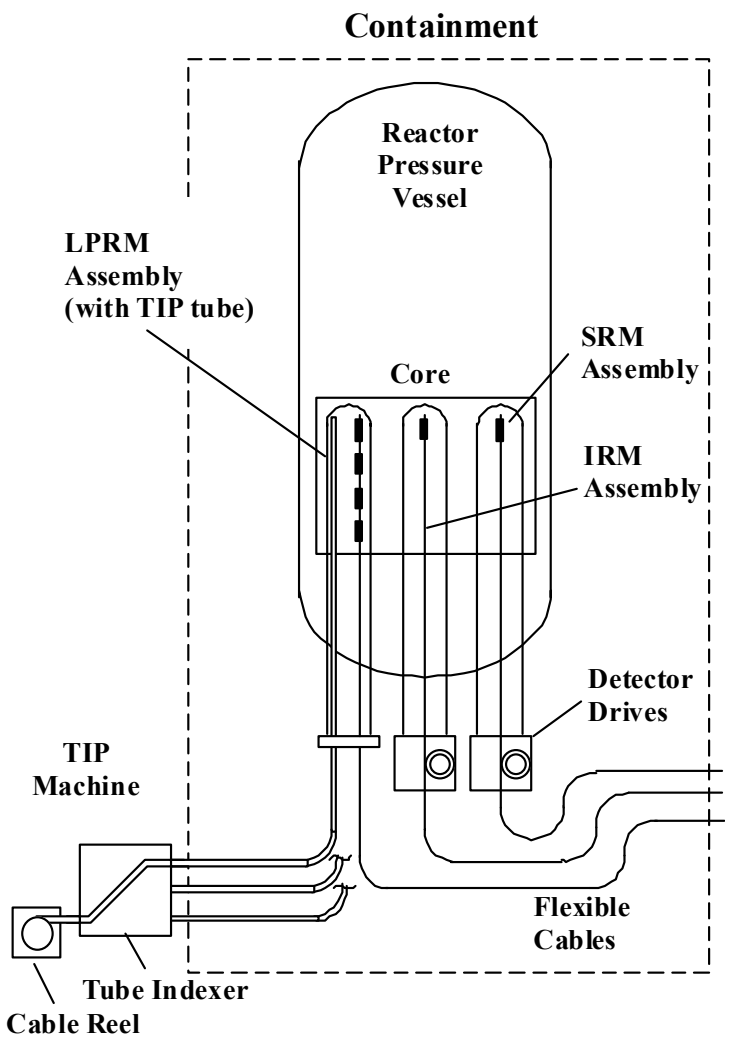
Neutron Monitoring System – Nonsafety-Related Subsystems

> Automated Fixed In-core Probe (AFTIP) (that replaces TIP system)

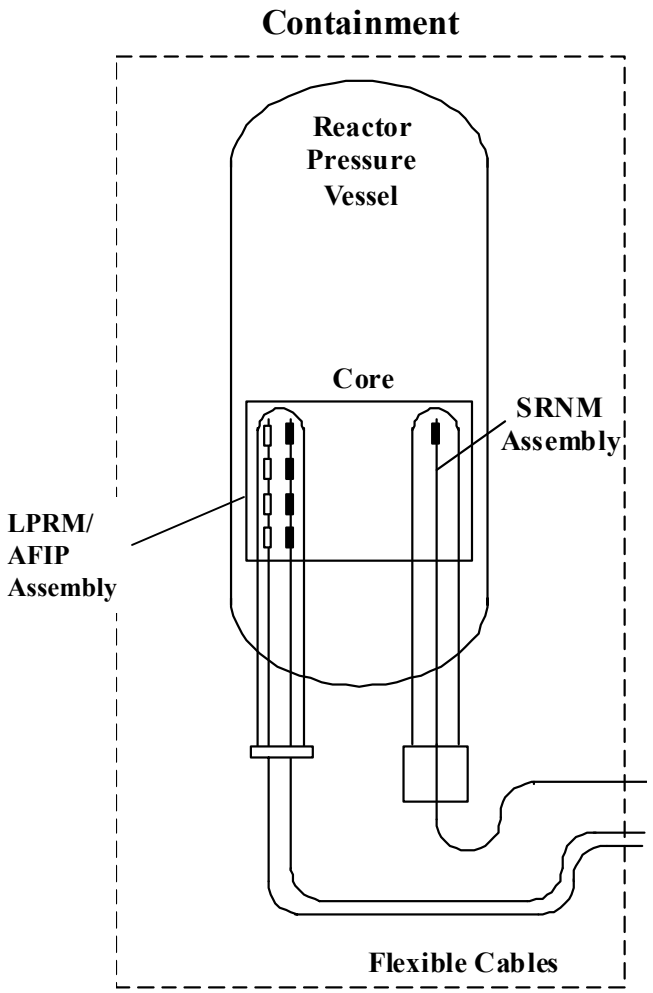
>Multi-Channel Rod Block Monitor (MRBM)

- Multiple regional RBMs based on regional LPRM measurements
- Safety Limit MCPR Protection
- RBM algorithm has same design concept as BWR 5 RBM
- MRBM has same design as in ABWR

Incore Instrumentation



Conventional BWR



ESBWR

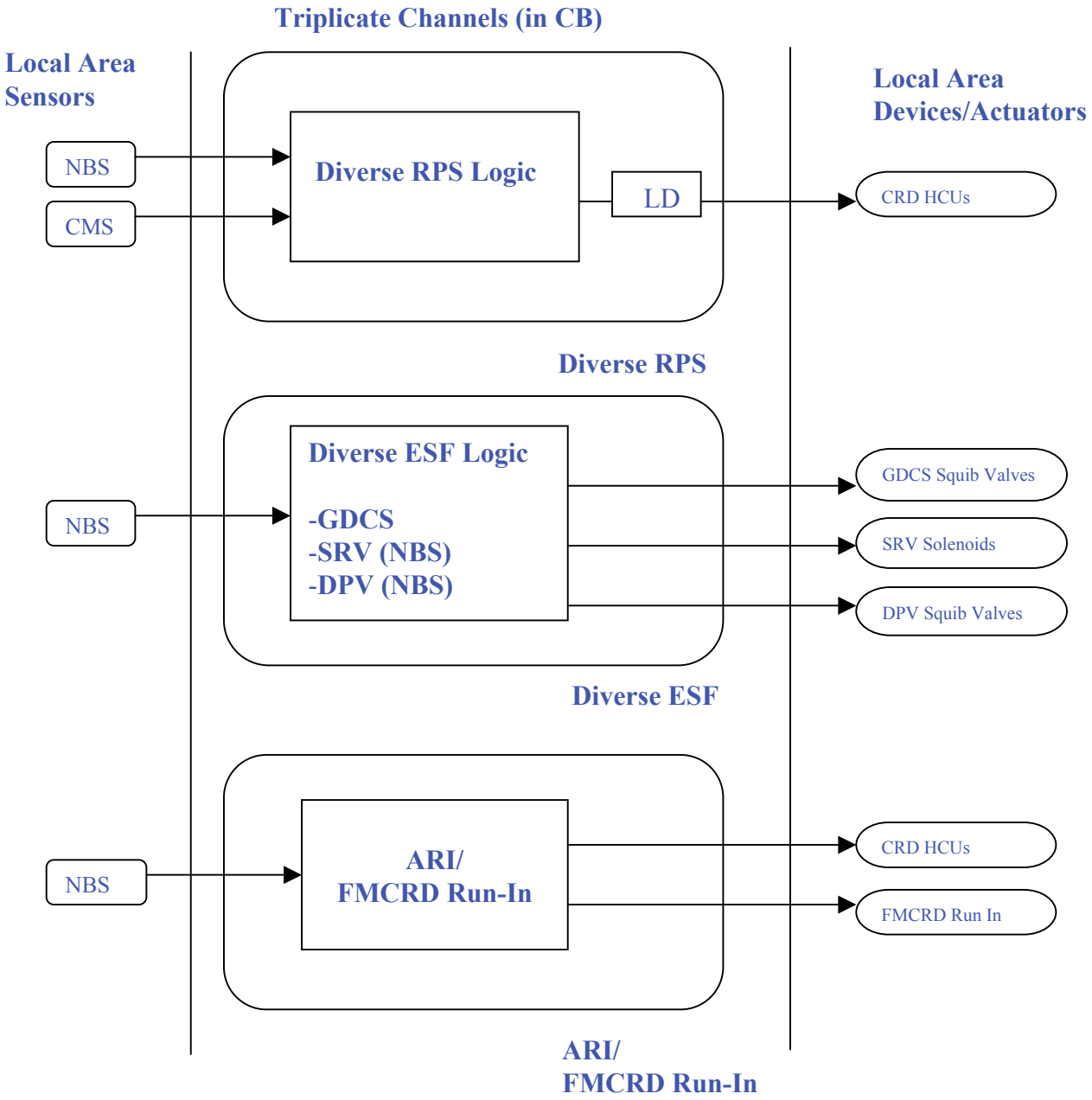
ESBWR Automation

- Plant operation is automated:
  - From cold startup to rated power
  - Full power operation
  - From rated power operation to plant shutdown
- Nonsafety-related I&C provides automatic startup/shutdown algorithms and controls, regulates reactivity during criticality control, provides heatup & pressurization control,
- No safety-related RPS/ECCS or nonsafety rod block protection is lost in automation
- Any control rod block (I&C self-check failure) or operator decision can convert the plant operation to manual operation
- Reduces operator burden by carefully selected “breakpoints” requiring operator attention (“acknowledgment”) between automation sequences
- Control algorithms proven in ABWR

Diverse Instrumentation & Control Systems

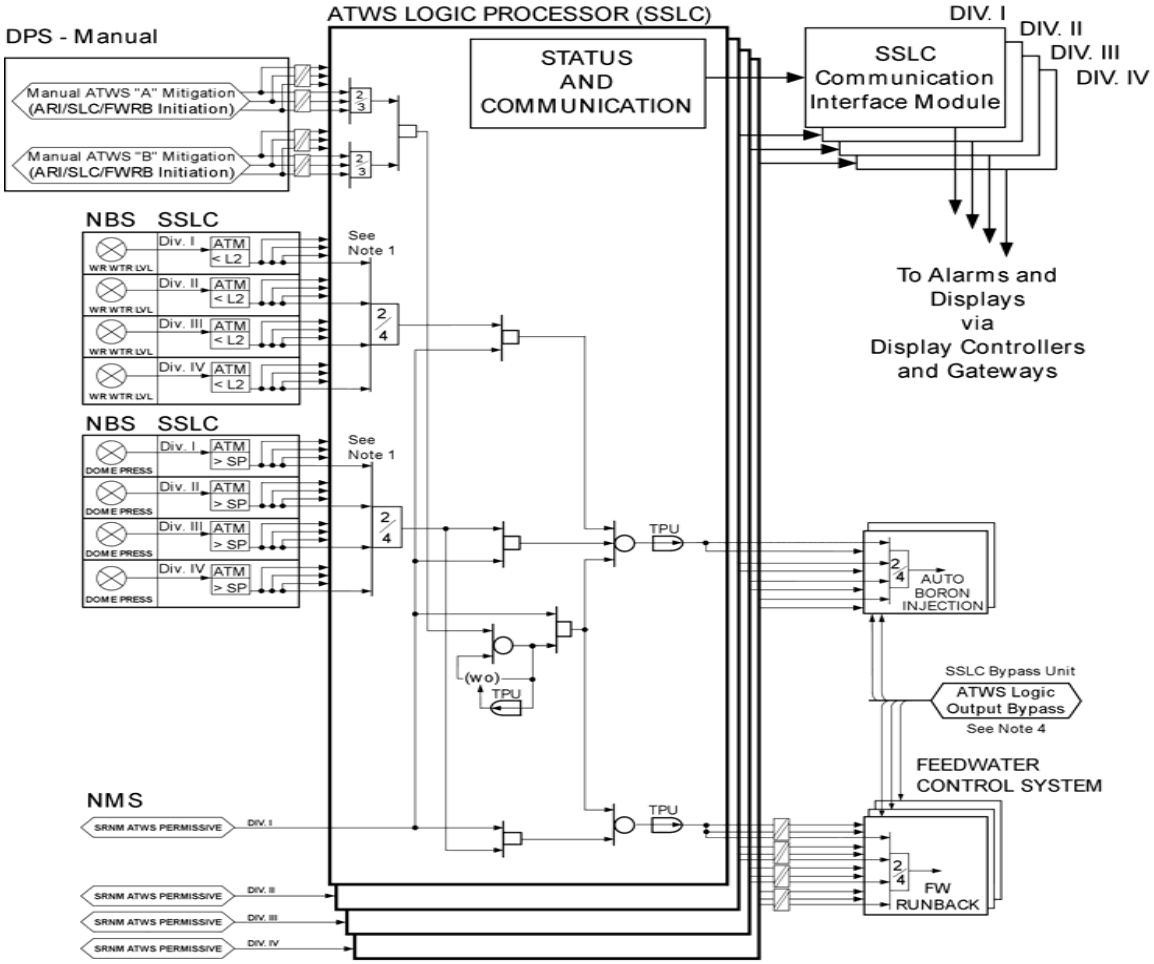
- Safety-related "ATWS/SLCS" Logic (Liquid boron injection)
  - > Four Class 1E divisions within SSLC
  - > Manual control available
- ESBWR "Diverse protection system"
  - > A subset of RPS protection logics that provide diverse means to scram the reactor using separate and independent sensors, hardware and software from the primary RPS.
    - – single failure proof
  - > A subset of ESF initiation logics that provide diverse means to initiate certain ESF functions using separate and independent sensors, hardware and software from the primary ESF systems.
    - – ADS and GDCS
    - – single failure proof
  - > A set of alternate rod insertion (ARI) and associated logics (e.g., control rod run in) through alternate means by opening the three sets of air header dump valves of the Control Rod Drive system. (also part of the ATWS mitigation function, same as ABWR)
  - > Does not degrade primary scram/ECCS reliability
  - > Manual control available

Diverse Protection System



RPS = Reactor Protection System
NBS = Nuclear Boiler System
CRD = Control Rod Drive (System)
CMS = Containment Monitoring System
RTIF = Reactor Trip & Isolation Function
ESF = Engineered Safety Feature
GDCS = Gravity Driven Cooling System
ICS = Isolation Condenser System
ADS = Automatic Depressurization System
SRV = Safety Relief Valve
DPV = Depressurization Valve
ARI = Alternate Rod Insertion
FMCRD = Fine Motion Control Rod Drive
LD = Load Driver
HCU = Hydraulic Control Unit

ATWS/SLCS Logic



NOTES:

1. DIVISION-OF-SENSORS BYPASS INPUTS AND LOGIC NOT SHOWN.
2. THE ATWS LOGIC PROCESSOR SHALL INCLUDE DIVISION-OF-SENSORS BYPASS EXCLUSIONARY LOGIC THAT RESULTS IN A "NO BYPASS" CONDITION FOR ALL DIVISIONS IF TWO OR MORE BYPASS INPUTS ARE RECEIVED.
3. THE ATWS LOGIC PROCESSOR SHALL INCLUDE DIVISION-OF-SENSORS BYPASS LOGIC THAT BYPASSES TRIP INPUTS FROM ALL SENSORS IN ONE DIVISION WHEN DIVISION-OF-SENSORS FOR THAT DIVISION IS PRESENT.
4. SEE SSLC LOGIC DIAGRAM FOR ATWS OUTPUT BYPASS LOGIC.
5. SLC FUNCTIONS IN ATM NOT SHOWN. SEE SLC LOGIC DIAGRAM.

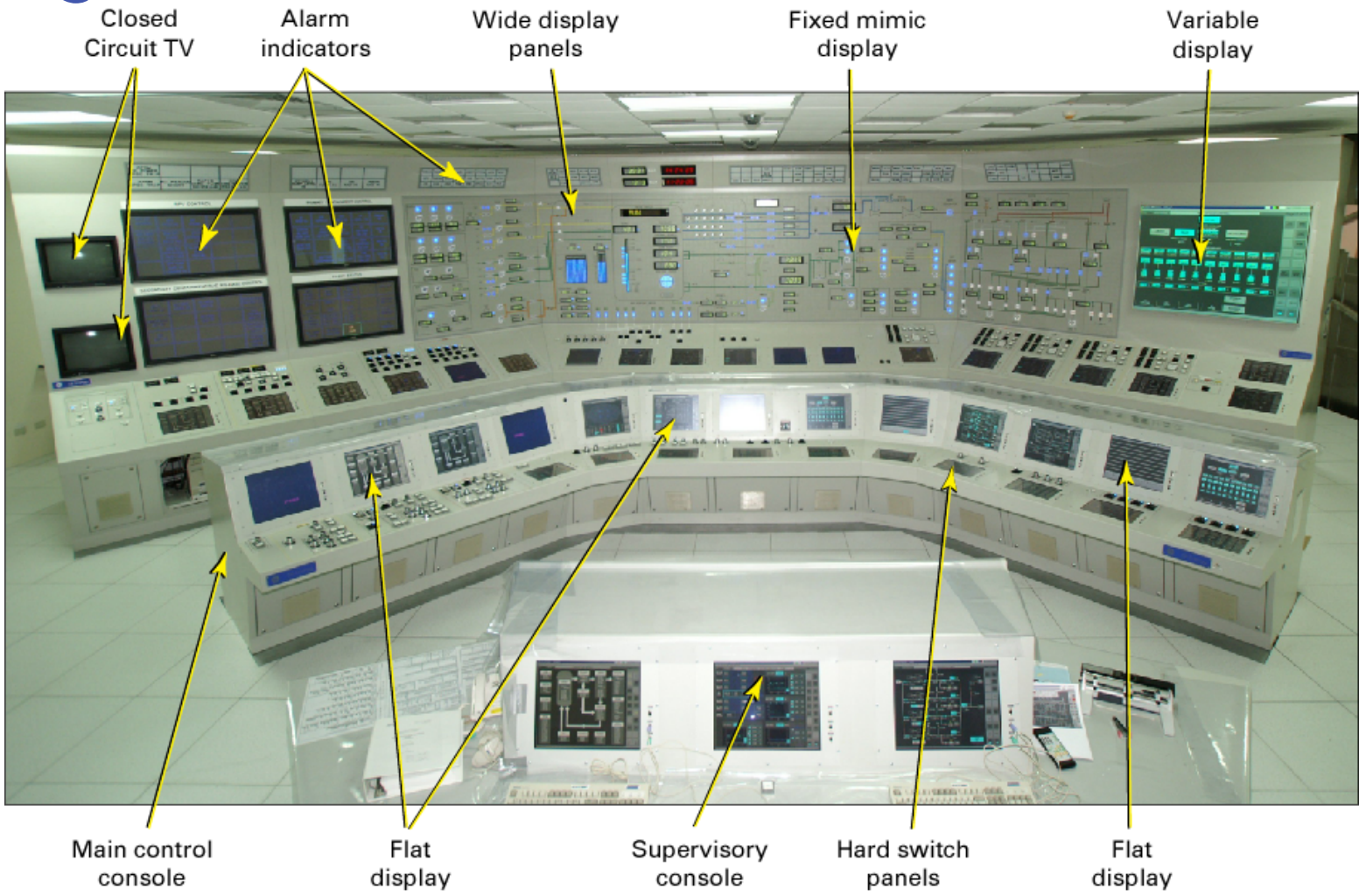
Summary of ESBWR I&C Characteristics

- ESBWR's digital I&C design is based on similar digital I&C framework, design, and hardware/software platforms as ABWR. The ABWR digital I&C design has been in operation and in construction (with hardware/software in fabrication/testing) – proven system and hardware/software designs
- Automation implemented similar as ABWR
- Minimized hardwired cables/utilize fiber optics similar as ABWR
- Digital Remote Shutdown System capable of full plant control and enhances EOP utilization
- Enhanced "diverse protection and actuation" capability in compliance to BTP HICB - 19
- AFIP to replace the TIP system
  - – simplified operation and reduced personnel radiation dosage.
  - - eliminated TIP containment penetrations
- The ESBWR I&C design will comply with updated or newly developed regulatory requirements such as BTP-14 (Software Life Cycle Design Process), BTP-19, as well as RG1.152.

ESBWR Man-Machine Interface (MMI)

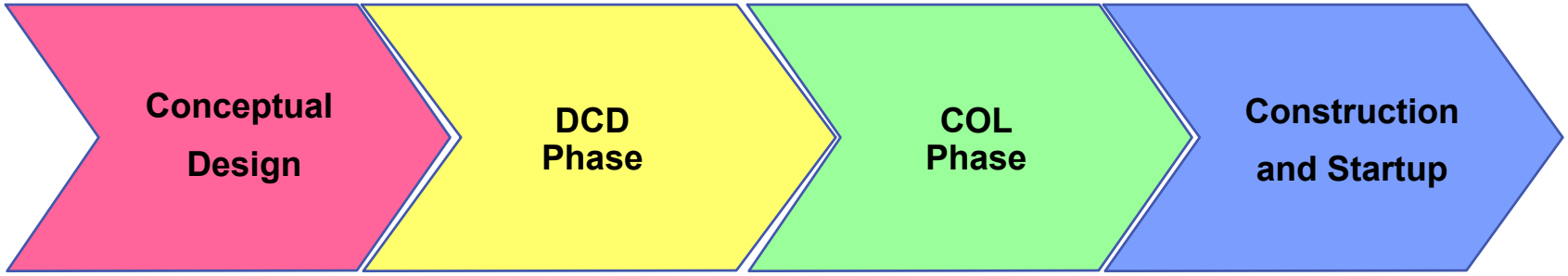
- Design in accordance with HFE principles / plan
- Alarms annunciated and prioritized per plant condition
  - > Reduces Operator burden in an event
- Alarm displays keyed to specific alarm response procedure
- Main mimic incorporates all SPDS control parameters and many RG 1.97 parameters
  - > Operator is aware of validation status of signals on mimic and displays
- Recording includes sequence of events, transient recording for planned and unplanned transients

Lungmen Simulator



Planning and Analysis	Design	Verification and Validation	Implementation and Operation
HFE Program Management	Human-System Interface Design		Design Implementation
Operating Experience Review			
Functional Requirements Analysis And Function Allocation	Procedure Development	Human Factors Verification & Validation	
Task Analysis			Human Performance Monitoring
Staffing & Qualification	Training Program Development		
Human Reliability Analysis			

ESBWR HFE Implementation



Conceptual Design

- Passive Safety
- 72 hour "Grace Period"
- Severe Accident Counter-measures

DCD Phase

- HFE Program Management Plan, adding:
  - OER Plan
  - HRA Plan
  - Staffing and Qualifications Plan
  - Training Program Plan
  - HPM Plan
- OER
- Function Allocation
- Task Analysis

COL Phase

- Staffing and Qualifications
- Human Reliability Analysis
- Human-System Interface Design
- Procedure Development
- Training Program Development

Construction and Startup

- Human Factors Verification and Validation
- Design Implementation
- Human Performance Monitoring